

Docket JP920030162US1

Appl. No.: 10/698,197
Filing Date: October 31, 2003**REMARKS****Posture**

The original application, filed October 31, 2003, included claims 1-35. An Office action of June 14, 2007, presented a restriction requirement with claims grouped as claims 1-11, 13-23, and 25-34 in Group I, and claims 12, 24, and 35 in Group II. In a Response to Restriction Requirement of July 6, 2007, Applicant elected to prosecute the claims in Group I, claims 1-11, 13-23, and 25-34, without traversal, wherein the claims of Group I were to be prosecuted alone (and the claims of Group II were to be correspondingly withdrawn).

Informalities

In the present, nonfinal Office action of September 27, 2007, Examiner objects to claims 2, 14, 26 for minor informalities.

Specifically, in each respective one of the cited claims Examiner requests that Applicant change "... administrator any data packets are ..." to read "... administrator of any data packets that are..." Likewise, in each respective claim Examiner requests that Applicant change "... transport layer terminate ..." to read "... transport layer to terminate ..." Applicant has responsively amended claims 2, 14 and 26 in accordance with Examiner's request.

Examiner also objects to claims 6-8 on grounds that they have improper dependency numbering. Applicant responsively herein amends claim 1 to incorporate claims 6 and 8, cancels claims 6 and 8, and amends claim 7, thereby overcoming the objection.

Claim Rejections - 35 USC § 101

Claims 25-34¹ stand rejected under 35 U.S.C. 101 on grounds that the claimed invention is directed to nonstatutory subject matter. In this regard, Examiner also cites MPEP 2106, Section IV, C. Specifically, the Office action points out that instructions in-and-of themselves have no ability to perform the claimed actions of "detect", "determining", etc., and that the instructions must be embodied where they are executed by some type of processing system.

¹ Although the Office action states that the rejection applies to claim 35, Applicant takes the rejection as actually applicable only to claims 25-34, since language from these claims is recited in the rejections and since claim 35 has been withdrawn.

Docket JP920030162US1

Appl. No.: 10/698,197
Filing Date: October 31, 2003

Furthermore, Examiner requests that Applicant change "computer- readable medium" to "computer-readable storage medium."

Applicant herein amends claims 25-34 to overcome the rejections.

Claim Rejections - 35 USC § 112

Claims 11 and 23² stand rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. Specifically, the Office action asserts, with regard to "generating a fake response," that since the claims are silent as to what action gives rise to this response, the claims are vague and unclear.

To overcome the rejection, Applicant herein amends claims 11 and 23 to recite "generating fake, network-accessible services." No new matter is added, since the original application provides support: Published application 20050108393, paragraphs 0070-0071.

Claim Rejections Based on Prior Art

Claims 1, 3-11, 13, 15-23, 25 and 27-34 stand rejected under 35 U.S.C. 102(b) as being anticipated by US Patent No 6,279,113 (**Vaidya**). Claims 2, 14, 26 stand rejected under 35 U.S.C. 103(a) as being unpatentable over **Vaidya** in view of US Patent No 7,185,368 (**Copeland**).

Claims 1, 13 and 25

Applicant hereby traverses the rejections of originally submitted claims 5, 6 and 8; 17, 18 and 20; and 29, 30 and 32. To overcome the rejections, Applicant herein submits amendments to claims 1, 13 and 25 to incorporate claims 5, 6 and 8; 17, 18 and 20; and 29, 30 and 32, respectively, and to recite additional limitations more particularly pointing out patentable features of the present invention. (Accordingly, Applicant herein cancels originally submitted claims 5, 6 and 8; 17, 18 and 20; and 29, 30 and 32.)

² Although the Office action states that the rejection applies also to claim 34, Applicant takes the rejections as actually applicable only to claims 11 and 23, since claim 34 does not mention a "response."

Docket JP920030162US1

Appl. No.: 10/698,197
Filing Date: October 31, 2003

Regarding originally submitted claim 5, the language of which is now incorporated into claim 1, the Office action asserts that Vaidya, column 7, lines 11- 40, teaches at least one application receive queue functions intermediate said transport layer and said application layer. However, the cited passage makes no mention nor suggestion whatsoever of a queue that functions intermediate said transport layer and said application layer.

Likewise, regarding originally submitted claim 6 the language of which is now incorporated into claim 1, the Office action asserts that Vaidya, column 7, lines 11-24, teaches said scanning step is carried out between said transport layer and said at least one application receive queue. However, the cited passage makes no mention nor suggestion whatsoever of a scanning step that is carried out between a transport layer and a receive queue.

And regarding originally submitted claim 8, the language of which is now incorporated into claim 1, the Office action asserts that Vaidya, column 7, lines 31-40, teaches said scanning step is performed on data packets from said at least one application receive queue. However, the cited passage makes no mention nor suggestion whatsoever of a scanning step that is performed on data packets from a receive queue.

To all the more certainly point out and more particularly claim these distinctions, claim 1 is further amended to state that the method includes "scanning data packets *by a first computer system to which the data packets are directed, wherein the scanning includes the computer system processing the packets by a transport layer of a network protocol associated with said communications network using signatures from a repository of said signatures*" and to state that the "at least one application receive queue (ARQ) . . . *provide[s] a queue for data from the data packets to a first application on the first computer system, wherein the scanning of the respective data packets occurs before the first application receives the data from the respective data packets*" (emphasis added). The cited references do not teach or suggest this.

No new matter is added, since the original application provides support for the amendments. Published application 20050108393, paragraph 0033 ("The embodiments of the invention disclose a "Host-based Network Intrusion Detection System" (HNIDS) that allows each host in a network to run network intrusion detection software, in a manner analogous to anti-virus software. The architecture enables every system on the network to act as an autonomous entity in detecting and managing intrusions."); paragraph 0031 ("Deploying a

Docket JP920030162US1

Appl. No.: 10/698,197
Filing Date: October 31, 2003

Network Intrusion Detection System (NIDS) on every host in a network substantially increases the security of the entire network. The embodiments of the invention disclose architectures that differ from existing NIDS architecture in that HNIDS architecture does not work on passive protocol analysis using promiscuous mode capture, thereby facilitating the use of NIDS on every host in the network.”); paragraph 0061 (“FIG. 6 is a flow diagram summarizing the process 600 for the embodiment of FIG. 5. A packet is received by the HNIDS 530 from the transport layer 516 in step 601.”); paragraph 0056 (“The Application Receive Queue (ARQ) is the queue from where the application takes its data,” i.e., claimed “first application” to which is directed the data of a data packet.); paragraphs 0047-0048 (Scanning is done by intrusion detection software that is independent of the application to which the data packet is directed, i.e., “As the HNIDS 100 is local to a system, the HNIDS 100 does not directly interface with the outside world. The HNIDS 100 can be a separate application that is installed on the host, or the HNIDS 100 can be part of the host’s network implementation.”), see also paragraphs 0061 and 0063 (indicating that the data is directed to an application that is different than the intrusion detection software that does scanning, since in the embodiment of FIG. 6, “If the data is malicious (YES), the data is not passed to the application 520” and in the embodiment of FIG. 7, “The HNIDS 730 of the further embodiment monitors the Application Receive Queue (ARQ) 718 . . . the HNIDS 730 may inform/instruct the application 720 so as not to process the packet.”).

For the above reasons, Applicant submits that amended claim 1 is patentably distinct with regard to the asserted references. Amended claims 13 and 25 have language similar to amended claim 1, each according to the form of the invention they claim. Accordingly, Applicant submits that claims 13 and 25 are allowable for reasons as set forth above regarding claim 1.

Claims 11 and 23

With regard to claims 11 and 23, the Office action asserts that Vaidya, column 11, lines 52-65, teaches generating fake responses. Amendments to these claims are herein submitted (as described herein above with regard to rejections under 35 USC 112, second paragraph), so that the amended claims state that the target computer system generates fake, network-accessible services. Applicant submits that the relied upon references do not teach or suggest this.

Docket JP920030162US1

Appl. No.: 10/698,197
Filing Date: October 31, 2003**Claims 2, 14 and 26**

Regarding claims 2, 14 and 26, the Office action asserts that Vaidya, column 6, lines 21-25, teaches said at least one action is selected from the group consisting of: "interrupting transmission of any data packets determined to be malicious to said application layer of said network protocol." Applicant herein amends the claims to state that "the interrupting is performed prior to the first application processing the malicious data packets." Applicant submits that the relied upon references do not teach or suggest this.

No new matter is added, since the original application provides support for the amendment. Published application 20050108393, paragraphs 0061 and 0063 (indicating that the data is directed to an application that is different than the intrusion detection software that does scanning, since in the embodiment of FIG. 6, "If the data is malicious (YES), the data is not passed to the application 520" and in the embodiment of FIG. 7, "The HNIDS 730 of the further embodiment monitors the Application Receive Queue (ARQ) 718 . . . the HNIDS 730 may inform/instruct the application 720 so as not to process the packet.").

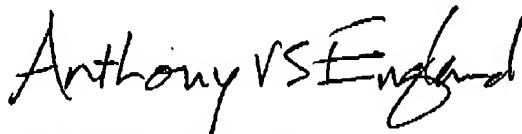
Claims 3-10, 15-22, and 27-34

Claims 3-10, 15-22, and 27-34 are allowable at least because they depend on respectively allowable claims.

REQUESTED ACTION

Applicant submits that the claims as submitted herein are patentably distinct, and hereby requests that Examiner grant allowance and prompt passage of the application to issuance.

Respectfully submitted,



Anthony V. S. England
Attorney for Applicant
Registration No. 35,129
512-477-7165
a@aengland.com